EXHIBIT A

FD-1057 (Rev. 5-8-10)

UNCLASSIFIED

FEDERAL BUREAU OF INVESTIGATION

Electronic Communication

Title: (U) Computer Scientist analysis of Washburn DDoS logs

Date: 01/14/2016

CC: Brian W. Behm
MP-CY-1 (OST)

From: MINNEAPOLIS
MP-CY-1
Contact: TYRA JAMES T, 763-569-8389

Approved By: SSA Michael J. Krause

Drafted By: TYRA JAMES T

Case ID #: 288A-MP-6766321 (U) UNSUB;
Victim: Washburn Computer Group;
Computer Intrusion - Criminal

Synopsis: (U) Washburn Group analysis notes of BlockDos logs and LiquidWeb tickets, approximate dates July 1st - October 20, 2015.

Full Investigation Initiated: 11/17/2015

Details:

Washburn Group Analysis Notes

Prepared by: James Tyra
10/29/2015

People

1. Washburn Group -Main victims of attack. Potential former disgruntled employee. Operates simple public info website, not sophisticated.
2. Logicnet.us - Provided website services to Washburn Group (??).
3. LiquidWeb - Contracted by logicnet.us for actual site / server hosting.

UNCLASSIFIED

Title: (U) Computer Scientist analysis of Washburn DDoS logs
Re: 288A-MP-6766321, 01/14/2016

Events

On July 30th roughly 16:14 attack starts. Liquid Web employee informs Washburn Group that DoS attack to 67.227.188.185 (DNS Name: host1.wcgpdb.com). Liquid Web "null routes" traffic, Attack stops, re-routes traffic, attack continues. This goes off and on 5-6 times until July 30th, 22:30. Attacks range from 226Mbps to 2.5Gbps. No mention of type of attack, besides being "Very Distributed" and "No common source port".

On July 31st ,15:07 a Liquid Web employee null routes 67.227.188.185 again, this time claims 4.4Gbps "DNS reflection attack".

On August 6th, 23:38 Liquid Web detects a 1.4 Gbps NTP DDoS (source port 123) to 67.227.188.185. Null routes traffic for ~30 minutes. Traffic dies down on August 7th 00:01 and traffic is routed back to normal.

On August 10th, 15:33 a 1.72 Gbps Source port 0/DNS Amplification attack occurs. Over next 3 days Attack continues on and off, stops when null - routed and continues when re-routed.

On August 11th, 20:52 PM CDT, ken@washburngrp.com receives e-mail from Loren Stoltenberg <loren_stoltenberg@yahoo.com>, asking how things are going. E-mail analysis indicated originating e-mail IP unknown (not shown). Email was likely sent from Yahoo web mail servers. Legal process to obtain original IP possible.

On August 12th, 18:26 a new IP is added to server and public DNS is updated to reflect that.

- Wcgpdb.com - 67.225.131.73
- Washburngrp.com - 67.225.131.74

On August 13th, 07:10 another attack is detected by liquid web, targeting 67.225.131.74. Liquid web starts recommending DDoS protection services.

On August 13th, 17:33 the DDoS attack picked back up. 40Mbps Syn Flood attack.

On August 14th, DDoS mitigation with Incapsula is setup and installed. LiquidWeb installs apache .htaccess rules to limit access to Incapsula only servers.

Title: (U) Computer Scientist analysis of Washburn DDoS logs
Re: 288A-MP-6766321, 01/14/2016

On October 6th 2:13 PM CDT ken@washburngrp.com receives e-mail from Loren Stotlenberg lorenstoltenberg15@gmail.com, again asking if they need any IT support. Gmail does not put original IP in e-mail headers, need legal process to obtain.

Random Analysis Notes

- Only 2 sites were hosted on the VPS by logicnet.us
- DDoS starts at 06/Oct/2015:16:15:56 -0400 according to the logs. Prior to this there were <3 human visits to the site from Aug 26 - Oct 6th.
- IP 70.191.120.105 is of interest. Cox communications IP in Ohio. Taken from BlockDOS logs.
- IP 192.154.137.65 is of interest. Owned by Privax AKA Hide My Ass VPN service. This ip does actual real fetches of homepage (gets css,js,etc), (see: 06/Oct/2015:16:53:48), then DoS like fetches (see: 06/Oct/2015:16:26:14 -0400)
- 2 IP's above hit server at almost exact same time frame (see: 06/Oct/2015:16:53:43)
- IP 14.192.128.179 visits the site on Aug 26th, then again during DDoS attack on 06/Oct/2015:16:54:23 -0400

Questions

- Did anyone at Washburn Group, Logicnet.us or Liquid Web use the tool "StatusCake"? This is a website monitoring service that appears to be active at various times.
- Did anyone at Washburn Group, Logicnet.us or Liquid Web use the tool "Pingdom"? This is a website monitoring service that appears to be active at various times. Specifically it started monitoring 5-10 minutes into the DDoS attack on October 6th.
- What (if any) connection is there to Ohio?
- Are logs available for any of the other attacks? Specifically the SYN Flood attack referenced on Adam Kaminski of Liquid Web support ticket 626995 on August 13th 2015?

Title: (U) Computer Scientist analysis of Washburn DDoS logs
Re: 288A-MP-6766321, 01/14/2016

♦♦